

REMARKS

Applicants have thoroughly considered the Examiner's remarks in the November 4, 2008 Office action and have amended the application to more clearly set forth aspects of the invention. Claims 1, 4-7, 10-13, 16-17, 19-24, 27-28, 30-31, and 36-41 are presented in the application for further examination. Claims 1, 11, 24, and 28 have been amended by this Amendment B. Claim 14 and 15 has been canceled by this Amendment B. Reconsideration of the application claims as amended and in view of the following remarks is respectfully requested.

DRAWINGS

Applicants respectfully request that the Examiner now have the drawings as originally filed reviewed and accepted.

Claim Rejections under 35 U.S.C. § 102

Claims 1, 4-7, 10-17, 19-24, 27-28, and 30-31 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pub. No. 2002/01447810 (hereinafter "Traversat"). Applicants respectfully disagree and submit that Traversat fails to disclose each and every element of the claims.

Claims 1, 4-7, 10, and 36-41

Amended independent claim 1 recites a method of providing from a centralized location access control to a resource for one or more users, with the method comprising, among other things:

receiving **at the centralized location** an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users as part of an organization model, wherein said authorization data is required by a second entity for allowing the first entity to access a resource controlled by the second entity;

responsive to the received authorization request, issuing the authorization data **from the centralized location** to the first entity, wherein the first entity provides the issued authorization data to the second entity, said authorization data including an expression identifying the resource by a resource name and by at least one property associated with the resource to conditionally define access to the resource, said authorization data further including validation information;

receiving **at the centralized location** a validation request from the second entity

to validate the issued authorization data that was provided to the second entity by the first entity; and

responsive to the received validation request, validating the issued authorization data based on the validation information included therein;

sending from the centralized location a response to the second entity indicating a determined validation status responsive to said validating the issued authorization data.

In order to provide a single and consistent point of access control for the management of resources, the method of claim 1 provides access control in a centralized location that is accessible by other entities (e.g., the first and second entities of claim 1). FIG. 1 of the present application illustrates an exemplary system embodying aspects of the method of claim 1. In this example, a client application 106 (a "first entity") requests a resource from an affiliate service 108 (a "second entity"). The affiliate service requests authorization data from the client application before allowing access to the resource. In response to the request, the client application requests a user authentication token from the **centrally located** authorization service 102. The authorization service receives the request to issue the token for the user based on access rights associated with the user, and in response to the request, issues the authorization data token with the token including a resource name and at least one property associated with the resource that defines what access the user has to the resource. Once the client application has received the token, the client application sends the token to the affiliate service. The centrally located authorization service in FIG. 1, embodying aspects of amended claim 1, receives a validation request from the affiliate service to validate the user's token and validates the token for the affiliate service in response to the validation request. The authorization service then sends a response to the affiliate service indicating a validation request status. In this manner, the resources of one or more affiliate ("second entity") services can be centrally controlled and managed in response to one of more user ("first entity") requests to access the resources, making access control administration manageable and scalable, while improving security by increasing the granularity and manageability of access control. Security is improved for the second entity, as the first entity must validate itself to a known authorization service trusted by the second entity before the first entity is allowed to communicate directly with the second entity resource. Requests for access to second entity resources are first directed to the authorization service, and if the first entity cannot validate itself to authentication service, the first entity is prevented from

accessing the desired second entity resource. See Application at paragraphs [0006], [0045], [0047], and [0102]; FIG. 1.

Applicants submit that the cited reference fails to show all of the elements of amended independent claim 1. According to the Examiner, Traversat discloses a method of providing access to a resource for one or more users, with the method disclosing each element of claim 1. However, Traversat does not disclose each and every element of amended independent claim 1. Traversat states:

[0065] Embodiments of an open network computing platform designed for peer-to-peer computing are described. The network computing platform may be referred to as a peer-to-peer platform. The peer-to-peer platform may be used to build a wide range of distributed services and applications in which every device is addressable as a peer, and where peers can bridge from one domain into another. The peer-to-peer platform may enable developers to focus on their own application development while easily creating distributed computing software that is flexible, interoperable, and available on any peer on the expanded Web. The peer-to-peer platform may enable software developers to deploy interoperable services and content, further springboarding the peer-to-peer revolution on the Internet. The peer-to-peer platform addresses the problems of prior art peer-to-peer systems by providing a generic and service-agnostic peer-to-peer platform that may be preferably defined by a small number of protocols. Each protocol is preferably easy to implement and easy to be adopted into peer-to-peer services and applications. Thus, service offerings from one vendor may be used, perhaps transparently, by the user community of another vendor's system.

Traversat merely describes a peer-to-peer ("P2P") platform, making improvements and extensions to P2P computing to overcome the limitations typically found in prior art P2P applications, specifically by enabling a wide range of distributed computing applications. Traversat, [0066]. To accomplish this goal, Traversat discloses a P2P networking platform consisting of computing devices acting as peer nodes (Traversat, Fig. 1B) that can discover each other, communicate with each other, and cooperate with each other to form peer groups and share network resources without requiring a central authority or server. Traversat, [0027], [0014]. Using this P2P model, Traversat further describes providing peer group services using **distributed, decentralized** methods.

However, the method of amended claim 1 recites, among other things, providing access control from a **centralized location** and "receiving at the **centralized location** an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users as part of an organization". The authorization data is issued from the **centralized location** in response to the received authorization request. Further, the method of claim 1 recites "receiving at the **centralized location** a validation request from the second entity to validate the issued authorization data that was provided to the second entity by the first entity", and in response, "validating the authorization data based on the validation information included therein" and "sending from the centralized location a response to the second entity indicating a determined validation status responsive to said validating the issued authorization data." Per the language of the claim, the elements of claim 1 occur at a centralized location. Traversat does not disclose or suggest a method of access control from a centralized location. In fact, Traversat teaches away from control access to resources from a centralized location – in Traversat, the P2P platform can define a set of core peer group service to be used to form and support peer groups, where the services provide the minimum services required to form a peer group, such as membership, access, and discovery services. Traversat, [0158]-[0159]. According to Traversat, the P2P platform core service should ideally be "100% decentralized and thus enable pure peer-to-peer network computing." Traverset, [0159]. Due to Traverset's distributed and decentralized nature, Traversat does not disclose or suggest a **centralized** method of access control as recite in amended independent claim 1.

In view of the foregoing, Applicants submit that amended independent claim 1 and its dependent claims 4–7, 10, and 36–41 are allowable for at least the reasons given above and rejection under 35 U.S.C. § 102(e) should be withdrawn.

Claims 11–13, 16–17, 19–23

With respect to the subject matter of amended independent claim 11 and its dependent claims 12–13, 16–17, and 19–23, the Examiner rejects claims 11–13, 16–17, and 19–23 for reasons similar to those given for the rejection of claims 1, 4–7, 10, and 36–41. Applicants respectfully disagree and submit that claims 11–13, 16–17, and 19–23 are allowable for at least the same reasons given above for the allowance of claims 1, 4–7, 10, and 36–41. As such,

rejection of amended independent claim 11 and its dependent claims 12–13, 16–17, and 19–23 under 35 U.S.C. § 102(e) should be withdrawn.

Claims 24 and 27

With respect to the subject matter of amended independent claim 24, the Examiner argues that Traversat discloses the components, on one or more computer-readable media, of claim 24. Applicants respectfully disagree and submit that Traversat does not disclose every element of the claim.

Amended independent claim 24 recites one or more computer-readable media having computer-executable components to control access to a resource by one or more users **from a centralized location**, said components comprising, among other things:

- an interface component adapted to receive **at the centralized location** an authorization request from a first entity to issue authorization data for the one or more users based on roles associated with the users, wherein said authorization data is required by a second entity for allowing the client to access a resource controlled by said second entity;

- an authorization component adapted to issue **at the centralized location** the requested authorization data for the users based on the roles associated with the users, said authorization data including an expression identifying a resource by a resource name and by a property associated with the resource and said authorization data including the validation information, wherein said interface component is further adapted to receive a validation request from the second entity, said validation request including the authorization data;

- a parser component adapted to retrieve validation information from the received authorization data; and

- a validation component adapted to evaluate the retrieved validation information, wherein the interface component is further adapted to send a response **from the centralized location** to the second entity indicating a validation status of the received authorization data responsive to said evaluating the retrieved validation information.

Applicants submit that claims 24 and 27 are patentable over Traversat for at least the same essential reasons given above for the allowance of claim 1, in that Traversat discloses a distributed and decentralized peer-to-peer networking technology and does not disclose or suggest components for controlling access to resources from a centralized location. As such, rejection of claims 24 and 27 under 35 U.S.C. § 102(e) should be withdrawn.

Claims 28 and 30–31

With respect to the subject matter of amended independent claim 28, the Examiner argues that Traverset discloses the authorization system of claim 28. Applicants respectfully disagree and submit that Traversat does not disclose every element of the claim.

Amended independent claim recites an authorization system **in a centralized location**, comprising, among other things:

- a memory area accessible from the **centralized location** for storing authorization data for use in providing a first entity access to a resource that is controlled by a second entity, said authorization data including an expression identifying the resource by a resource name and by at least one property associated with the resource; and

- a processor configured to execute computer-executable instructions for issuing from the **centralized location**, responsive to a request from the first entity, the authorization data for a user based on a role associated with the user and for validating, in response to a request from the second entity, the authorization data to provide access to the resource.

Applicants submit that claims 28 and 30–31 are patentable over Traversat for at least the same essential reasons given above for the allowance of claim 1, in that Traversat discloses a distributed and decentralized peer-to-peer networking technology and does not disclose or suggest components for controlling access to resources from a centralized location. As such, rejection of claims 28 and 30–31 under 35 U.S.C. § 102(e) should be withdrawn.

Conclusion

Applicants submit that the claims are allowable for at least the reasons set forth herein. It is felt that a full and complete response has been made to the Office action and, as such, places the application in condition for allowance. Such allowance is hereby respectfully requested.

Although the prior art made of record and not relied upon may be considered pertinent to the disclosure, none of these references anticipates or makes obvious the recited aspects of the invention. The fact that Applicants may not have specifically traversed any particular assertion by the Office should not be construed as indicating Applicants' agreement therewith.

Applicants wish to expedite prosecution of this application. If the Examiner deems the application to not be in condition for allowance, the Examiner is invited and encouraged to telephone the undersigned to discuss making an Examiner's amendment to place the application in condition for allowance.

The Commissioner is hereby authorized to charge any deficiency or overpayment of any required fee during the entire pendency of this application to Deposit Account No. 19-1345.

Respectfully submitted,

/Robert M. Bain/

Robert M. Bain, Reg. No. 36,736
SENNIGER POWERS LLP
100 North Broadway, 17th Floor
St. Louis, Missouri 63102
(314) 231-5400